Snap Inc.

Elizabeth Denham
Information Commissioner,
Information Commissioner's Office,
Wycliffe House, Water Ln, Wilmslow SK9 5AF

31 May 2019

Dear Commissioner,

Snap response to Age-Appropriate Design Code consultation

We welcome the opportunity to contribute to your Office's consultation on the Age-Appropriate Design Code. As you know, Snap remains committed to working in collaboration with your Office, the Government, and other stakeholders to help develop workable solutions in this policy area and are keen to share our thoughts with you on the draft Code you have produced.

The trust, safety and well-being of all Snapchatters is our utmost priority so we firmly share the Code's overall objective to ensure that children are safe online. With this in mind, there are three main areas that we would like to provide our feedback on in order to help ensure the Code effectively achieves its aims. These are:

1. Ensuring a principles-based and proportionate approach
2. Recognising the lessons of General Data Protection Regulation (GDPR)
3. Age-verification

This letter considers each of these areas in turn. Before doing so, I also wanted to set-out Snap's overarching approach to safety by design. We work to create a fun online space where users can enjoy high-quality curated content and interact predominantly with their closest friends. We appreciate this is not the case for many other consumer-facing applications and is a result of our unique approach to both privacy and design, so I wanted briefly to share our examples of best practice.

Snap's approach to design

We fully support the Code's objective for internet services and platforms to be designed with the best interests of children in mind. This is why in designing our own app, Snapchat, we have put a great deal of thought into how we can give young people the power to engage creatively, safely and positively when online.

The concept of appropriate design is foundational to Snapchat. We built Snapchat as an antidote to the context-less communication that defines “social media,” and we extend this approach to everything we do, including when it comes to design. Designing an app with well-being and creativity at the forefront creates a safer place for young people to engage positively with their friends and the world around them, whilst protecting them from the negative and unreliable content found on social media.

We develop and continually improve our products by listening to our community, seeking guidance from experts and working constructively with regulators and legislators in the UK and internationally. And indeed, these rules and initiatives that we build into our app’s design to protect young users do have a positive impact.

New features go through an intense product review process before they are released. From the earliest stages of development, a team of product and privacy attorneys works directly with our designers and engineers to develop safe, privacy-protective features that help Snapchatters live in the moment, learn about the world, and have fun together. Our product review process is guided by a few core principles: (1) we communicate honestly and openly with Snapchatters about how we use their information; (2) Snapchatters are in control of their information and how they express themselves; (3) we design with privacy in mind; and (4) Snaps and chats are designed to delete by default.

Given this approach, Snapchat’s design consciously encourages authentic relationships with a Snapchatter’s existing social circle. Unlike social media platforms, Snapchat does not have browsable public profiles including things like location, interests, or age. A Snapchatter’s friends list isn’t visible in the app, and users don’t see how many people view other Snapchatters’ Stories. And last, by default, you cannot receive messages from someone whom you haven't added as a friend on the app. Most interactions on Snapchat are between close friends.

To serve as a practical example of how our platform is designed with safety and privacy in mind - and how we accomplish providing special protection to children through adherence to our principles - I wanted to briefly touch on our approach to geo-location services given that they are a particular area of focus for your Office as detailed in the Code. Snapchat uses geo-location data to support several features, most notably Snap Map.

Snap Map is designed to open up a world of possibilities for our community, enabling friends to experience something new in the world every day. Through an interactive map interface, Snap Map shows users what’s happening nearby and around the world, anchored by the context of friends’ Bitmojis (avatar representations of users).

Given that location data and location-sharing are sensitive for younger individuals, Snap took appropriate steps in the design of Snap Map to ensure the particular risks to younger users would be mitigated. First, on Snapchat, location is off by default. Even if the Snapchatter has

already granted Snap location permission because he or she has used another location-based feature, such as our Geofilters, location-sharing on Snap Map is off by default.

Second, the first time someone uses Snap Map, a tutorial explains how to share one's location with specific friends or all friends, or remain hidden in what is called "Ghost Mode". The default is Ghost Mode (i.e., location-sharing is off). There is no option for users to share their location with users who are not friends.

Third, Snapchatters can update who among their friends can see their location at any time right from the settings gear in the Map. If users decide they would like to stop for any reason, they can simply toggle Ghost Mode on and they disappear from the Map within seconds. It is important to understand that Snapchat is not a broadcast platform, and does not give users the option to share their location publicly with a full contact list of people they may not know.

And fourth, if a Snapchatter who is sharing his or her location does not use the Snap Map for seven days, an in-app reminder will appear to indicate that location-sharing is on, and will continue every seven days that the Snapchatter does not use the Snap Map.

During the development of Snap Map, Snap privacy lawyers and engineers considered the design of the tutorial, the notices Snapchatters would see, the name of the setting (i.e., Ghost Mode), and other such aspects of the product design. This was to ensure that it would be understood by younger individuals, so they could make informed choices about whether to use the feature, whether to share their location and, if so, with whom to share it. Furthermore, in keeping with the principles of data minimization and purpose limitation in the GDPR, when younger individuals use Snap Map, Snap collects and uses the location data only for the purpose of providing the feature to the Snapchatter.

As we hope this example of our product development process illustrates, guided by strong principles, a company should be able to shape the way it provides special protections to children depending on the particular nature of its service. Specific tools such as balancing tests, checklists, and even legitimate interest assessments can be encouraged as mechanisms to tangibly address the Code's principles within the context of a company's product or feature design process. In this way, companies can demonstrate compliance with the Code. As described below, Snap is supportive of a principles-based Code, but this does not mean that the ICO cannot require some demonstrable evidence of compliance.

Ensuring a principles-based and proportionate approach

Given the fluid nature of the internet and the evolving way that consumers interact with online services, we are heartened to read the Code's acknowledgment that the standards espoused "are not intended as technical standards, but as a set of technology-neutral design principles and practical privacy features." Snap strongly agrees with this approach and - as the Code sets out - that "different services will require different technical solutions." The Code should be

flexible enough to adapt to the constantly changing nature of technology and service innovation in order to ensure that companies are able to meet the goal of keeping children safe while retaining the ability to innovate.

We believe, therefore, that the core principles outlined in pages 3-4 of the Code, which summarise the various areas that your Office would like industry to comply with when designing their services, provide the right level of detail and guidance for industry to follow, without falling into the trap of prescribing how to achieve those standards. The articulation of these standards alone would, in our view, suffice as the final Code. It allows the varied and myriad information society services (ISS) covered by the Code the right level of flexibility to apply the principles to their own services effectively and proportionately.

We believe the remainder of the Code is overly prescriptive in its application and too granular in its level of detail. For each of the 16 principles espoused in the Code, there is currently too great a focus on prescribing the ideal means to achieve the Code's intended outcomes. This would not allow for the myriad ways different companies could ensure compliance given the variety in the scope of service operations covered by the Code.

In taking a directive and overly prescriptive approach, the Code in its current form runs the risk of homogenising the online market to the detriment of innovation, limiting genuine attempts to ensure that services are designed with the best interest of the child in mind.

It is also vital, therefore, for the Code to be applied in a proportionate manner, depending on the size and type of business to which it is applicable, as well as the inherent level of risk of a particular service being provided. There is currently no mention of the impact of the Code's proposals on smaller online businesses. Many SMEs - which comprise a large part of the success of the online industry in the UK - will struggle to comply with the prescriptive and heavy-handed nature of many of the measures in the Code. It should not be that in attempting to curb the excesses of some of the largest platforms, the Code ends up unfairly benefiting them since they would be the only companies with the capability and resources to ensure compliance.

In summary, we urge the ICO to focus the Code solely on the "what" and to allow the "how" to be decided on by each individual organisation. Our simple recommendation would be to restrict the Code itself to pages 3-4, and if the ICO nevertheless wishes to issue any parts of the prescriptive remainder of the draft Code, to do so as non-binding guidance. This will help those companies and organisations who do not yet understand how to achieve such standards themselves while allowing those that do have the ability to decide for themselves how to comply. As mentioned in the section above, we believe that accompanying the principles in the Code with examples of concrete tools that could be used to execute on the principles - such as checklists, balancing tests, and risk assessments - would serve to focus companies on the specific ways they can protect children given what kind of product or service they offer.

Recognising the lessons of General Data Protection Regulation

For the reasons that we have outlined above, we would recommend that the ICO use the GDPR as its north-star for the effective design of the Code. GDPR is, rightly, heralded as an effective piece of regulation whose principles-based, horizontal nature means that it can be efficiently applied across a wide spectrum of industries and organisations across the European Union.

The GDPR already covers a number of the areas that this Code seeks to address, including transparency and proportionality. Consequently, we would urge the ICO to mirror the principles-based approach of the GDPR which provides sufficient flexibility for businesses to decide how they will comply with the standards set by the Regulation. We would also urge against any undermining of the delicate balance of interests carefully struck during the GDPR negotiations.

From the outset, Snap's privacy principles have aligned with those of the GDPR. As a result, Snap's preparation for the GDPR was less about implementing new compliance measures and more about enhancing our existing privacy programme.

The GDPR's principles and risk-based approach allow us to remain in compliance by continually improving our products in ways that make sense for our unique audience and platform. For example, rather than relying solely on a long-form privacy policy to provide Snapchatters with transparency, we were able to enhance user transparency by developing a series of innovative privacy-related Snaps in the Discover section of the app as well as short, plain-language privacy notices that can be easily read in-app. We believe that a principles-based approach guided by accountability grants us the flexibility to leverage our design resources to develop engaging privacy and safety-enhancing features that are embraced (rather than ignored) by our audience. These innovations would not have been developed under a prescriptive regulatory regime.

In summary, and simply put, regulators should set the principles to be adhered to and standards to be achieved, while companies and organisations should abide by those principles and achieve those standards in a way that best suits their operations.

Age verification

Snap acknowledges and shares your Office's desire to ensure that children are only accessing services appropriate for their age. This is why we design all of our services with age-appropriateness in mind. While we try to design features that function identically for all Snapchatters, our product attorneys understand that not everyone is the same and that some people — especially younger users — require extra protection. That's why some features — like Snap Map and Our Story — are designed to work differently (or not at all) for different users. Snap takes this issue very seriously and also recently responded to the Public Consultation of the Irish Data Protection Commission on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR ("Consultation"). We trust that our

response to that Consultation provides a complementary perspective on Snap's data practices and vision on children's privacy rights.

More broadly, Snapchat is designed to appeal to teen and adult audiences, and individuals under the age of 13 are not permitted to create Snapchat accounts. When registering an account, individuals are required to provide their date of birth and the registration process fails if a user is under the age of 13. We do not inform individuals that their registration failed due to their age and, on the web, we set a cookie to discourage repeated registration attempts. In all cases, we've designed our age-gating mechanisms to prevent the storage of information about under-13 individuals on our servers.

Snap also makes no effort to market Snapchat to children. It is not available in the "Kids" or "Family" sections of any app store. Snapchat is rated 12+ in the Apple app store and rated Teen in the Google Play store, putting parents on notice that Snapchat is not designed for children. These ratings reflect Snapchat's content, which is designed for teens and adults, and not children under 13 years of age.

However, we have concerns over the Code's proposals regarding "robust" age-verification mechanisms to distinguish children from adults. As you and your staff have previously acknowledged, to achieve age-verification of minors remains a complex goal. There are several unresolved legal and technical challenges.

For example, 'robust' age-verification would require the collection and retention of documents such as a copy of passports, driving licences or other documents. Your Office itself has said it has "significant concerns" that this data would be vulnerable to misuse and/or attractive to disreputable third parties. The alternative, usually using some form of data tokenisation through a trusted third party, is so far unproven at scale and cannot address (anti-)competitive issues of off-shore service provision. We are, nevertheless, committed to working with industry partners and the Government to find an industry-wide mandated solution that works internationally, but the timescales for this ambitious undertaking have to be realistic. Currently, it seems, political ambition and practical reality are out of step; the ICO's expert guidance in the matter would be beneficial for all sides.

We believe that the key to developing workable policy solutions in this area is to capture the widest possible community of stakeholders by focusing on the tightest pinch points in the value chain.

Interaction with either one of the two app stores is a key pinch point through which all users must pass before they can install apps on their phones. The two app stores are run by the two major operating system providers - Apple and Android. Introducing the two companies' comprehensive family suites of safety and wellbeing tools - age-gates, screen time limiters, downtime setting, monitoring app downloads and in-app purchases, white/black lists, etc - when signing up to the app stores would catch any new users who somehow fell through earlier

(and unavoidable) points-of-purchase gates. This appears to be the most viable opportunity for a robust and comprehensive age verification system to be developed and located. The more so, given the existence in both stores of credit card based verification for parents/carers.

Improving those existing gate-keeping mechanisms by which users already select and access pretty much all their apps would be a more effective, and scalable, tool to ensuring that children are only accessing apps which are both age-appropriate and acceptable to their parents/carers.

Expanding this thinking to a more holistic approach would also allocate responsibilities to other stakeholders in the value chain. Access to, and use of, applications require the user to pass through at least two technology “layers” before reaching the app store and operating system: the mobile operator’s data network and the hardware.

Children, by and large, do not buy their own phones. At the point of purchase, the purchaser (usually, the parent/carer) could be guided through the options to configure, in an age-appropriate manner, the phone’s safety parameters using the operating system tools provided, including linking to a family account with age-verification options controlled by a parent/carer for younger children.

Similarly, children, by and large, do not sign up or pay for mobile data subscriptions. At the point of purchase, small changes to the purchase flow could be designed so that the purchaser would be guided through the options to configure, in an age-appropriate manner, both the phone’s safety parameters using the operating system tools, as well as the mobile network operators’ own tools, such as age-gates, white/black lists and parental filters.

It is on these three key choke points that we feel the ICO’s attention should be focused when it comes to improving age-verification effectiveness. In particular, improving user understanding and take-up of the mechanisms by which children can access apps through the two app stores will be the most effective and scalable solution in the medium-to-long term.

I hope this letter is a useful contribution as you look to consider an Age-Appropriate Design Code. In closing, I would like to restate Snap’s willingness to continue to work with both you and HM Government more widely on this matter. Please do not hesitate to contact me if we can provide any further information or you would like to discuss any or all of the above points.

Yours sincerely,

Stephen Collins
Senior Director Public Policy International